EDR

Does Coro Endpoint Detection and Response (EDR) detect potentially malicious services running on devices?

Yes, the Coro EDR Allow/Block lists enable you to block the execution of unsafe processes. Blocking the execution of unauthorized or suspicious processes can help stop malware and other malicious software from running on the device.

For more information, see **EDR Block/Allow Lists**.

Can Coro Endpoint Detection and Response (EDR) block certain applications on devices?

Yes, the Coro EDR Allow/Block lists enable you to block the execution of applications.

For more information, see **EDR Block/Allow Lists**.

How does Coro Endpoint Detection and Response (EDR) isolate an infected device from a network?

When Coro isolates a device affected by a malicious process from the network, the device cannot communicate with any network or internet resource. However, the Coro process stays active, allowing the device to maintain communication with the Coro server for diagnostic purposes.

For more information, see **EDR processes**.

Does Coro Endpoint Detection and Response (EDR) provide the ability to disconnect/isolate a device from all internet activity and log in to the device using remote monitoring and management (RMM) software in order to diagnose?

Yes, selecting **Isolate from network** from a device on the **Devices** list isolates a device from networking and is only able to connect to the Coro Agent. After a device is isolated, a Coro admin can select **Open remote shell** to access a command prompt on the device, which allows remote command execution.

For more information, see **Device actions**.